EUROPEAN COMMISSION

Brussels, 30.9.2010
SEC(2010) 1123 final

COMMISSION STAFF WORKING DOCUMENT

SUMMARY OF THE IMPACT ASSESSMENT

Accompanying document to the

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on attacks against information systems, and repealing Council Framework Decision 2005/222/JHA

{COM(2010) 517 final}
{SEC(2010) 1122 final}

SUMMARY OF THE IMPACT ASSESSMENT

1. PROBLEM DEFINITION

The number of attacks against information systems has increased significantly since the adoption of the Framework Decision on attacks against information systems ('FD on attacks'). One of the leading Internet security firms reported that threats to confidential information (as opposed to publicly available information) increased considerably in 2008, rising from 624,267 to 1,656,227 identified new threats in 2008[1]. Moreover, a number of attacks of previously unknown large and dangerous scale have been observed, such as those in Estonia and Lithuania in 2007 and 2008 respectively. In March 2009, computer systems of government and private organizations of 103 countries were attacked by a network of compromised computers extracting sensitive and classified documents[2]. This was done through the use of 'botnets'[3], networks of infected computers that can be controlled from a distance. Finally, the world currently witnesses the spread of botnet called 'Conficker' (also known as Downup, Downadup and Kido), which has propagated and acted in an unprecedented scale and scope since November 2008, affecting millions of computers worldwide[4].

Secondly, insufficient co-operation between the Member States, and specifically law enforcement agencies and judicial authorities within the EU render a coordinated and effective response to these attacks difficult. Whilst the implementation report on the FD on attacks shows that a majority of Member States have put in place permanent contact points as required by Article 11 of the FD on attacks, problems persist as to their responsiveness and their capacity to react to urgent requests for cooperation[5].

The existence of a contact point is not a guarantee for its proper functioning. In their notifications to the Commission, a number of Member States indicated that although their respective contact points were in place, they were not operating 24 hours a day as required by the FD on attacks. This indicates that they cannot respond to urgent requests outside office hours. Public-private cooperation is often hampered by the low efficiency of contact points or their inability to deal with private sector requests for cooperation.

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, p.10.

2 ww.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail

3 The term botnet describes a network of computers that have been infected by malicious software (computer virus). Such network of compromised computers ('zombies') may be activated to perform specific actions such as attacks against information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'. The persons who control this centre are among the offenders, as they use the compromised computers to launch attacks against information systems. It is very difficult to trace the perpetrators, as the computers that make up the botnet and carry out the attack, might be located elsewhere than the offender himself.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html

5 Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems - COM(2008) 448.

Thirdly, there is still little data available about cyber attacks as well as the police and judicial follow-up of such attacks. Not all Member States collect data relating to cyber attacks. Those who collect them do so in a manner that does not allow for comparison due to diverging statistical methodologies among the Member States.

The victims of large-scale attacks against information systems include the general public consisting of the users of information systems, as well as central and local government, international organisations and private entities.

Attacks can be launched in third countries against targets within the EU, and the other way around.

2. SUBSIDIARITY

Cybercrime is a truly international problem, which can only rarely be fought in a mere national context. It is generally accepted that EU and international actions are needed in order to prevent and tackle it. Most attacks cross the borders of the EU. They affect all Member States, and there is evidence that a considerable proportion of them involve activities from one Member State to another. Information systems are often technically interconnected and interdependent across borders. The consensus among experts is therefore that international as well as EU actions are needed, and that the objective of effectively combating such crime cannot be sufficiently achieved by Member States alone.

A national approach to cybercrime runs the risk of producing a fragmentation and inefficiency across Europe. Differences in national approaches and the lack of systematic cross-border cooperation substantially reduce the effectiveness of domestic countermeasures. This is partly due to the interconnectedness of information systems as a low level of security in one country has the potential to increase vulnerabilities in other countries.

3. WHAT ARE THE OBJECTIVES?

3.1. General, specific and operational objectives

The overall goal of EU action is to combat and prosecute crime, organised or otherwise, in conformity with Article 67 of the Treaty on the Functioning of the European Union, by fighting against large-scale cyber attacks against information systems.

A **Specific objective: Prosecute and convict criminals responsible for large-scale attacks, through the approximation of criminal law in the area of attacks against information systems**

B **Specific objective: Improvement of cross-border cooperation between Law Enforcement Agencies (LEA's)**

C **Specific objective: To establish effective monitoring systems and data collection**

4. WHAT ARE THE POLICY OPTIONS?

4.1. Option (1) Status Quo / no new EU action

This option implies that EU will not take any further action to fight this particular type of cyber crime. Ongoing actions, in particular the programmes to strengthen critical information infrastructure protections and to improve public-private cooperation against cyber crime, would be continued.

4.2. Option (2) Development of a programme to strengthen efforts to counter attacks against information systems with non legislative measures

Non-legislative measures would, in addition to the programme for critical information infrastructure protection, focus on cross-border law enforcement and public-private cooperation, and should facilitate further coordinated action at EU level. A non legislative proposal could include actions such as the strengthening of the existing 24/7 network of contact points for law enforcement authorities; the establishment of an EU network of public-private contact points of cyber crime experts and law enforcement, and the elaboration of a standard EU service level agreement for law enforcement cooperation with private sector operators.

4.3. Option (3) Targeted update of FD on attacks to address the specific threat from large-scale attacks against information systems

This option implies an introduction of specific targeted (*i.e.* limited) legislation against particularly dangerous large-scale attacks against information systems. Such targeted legislation would be linked to measures to strengthen operational cross-border cooperation against attacks on information systems and at increasing already foreseen minimum penalties. This option would have the form of an update of the existing FD on attacks complemented by a number of non-legislative measures, such as enhancing preparedness, security and resilience of critical information infrastructure protection and the strengthening of instruments and procedures for cross-border law enforcement cooperation and best practice exchange.

4.4. Option (4) Introduction of comprehensive EU legislation against cyber crime

The identification of a need to take rapid action against the development of sophisticated attacks against information systems raises the question whether it would be appropriate to also introduce broader EU legislation on cyber crime in general. Such legislation would not only cover attacks against information systems, but also issues such as financial cyber crime, illegal web content, the collection/storage/transfer of electronic evidence and more detailed jurisdiction rules. Such EU legislation would be applicable alongside the Council of Europe Convention on Cybercrime, which would in particular be complemented with new provisions considered necessary within the EU.

4.5. Option (5) Update of the Council of Europe Convention on Cybercrime

This option would require substantial renegotiation of the current convention, which is a lengthy process and goes against the time frame for action that is proposed in the Impact Assessment. There seems to be no international willingness to renegotiate the Convention. It is therefore outside the required time frame for action to consider an update of the Convention a feasible option.

5. ASSESSMENT OF IMPACTS

Options	Economic impact	Social impact	Fundamental rights impact	Impact on third countries	Relevance for objectives A,B,C	Consistency with int'l law
Option 1: Status quo / no new EU action	0	0	0	-	0	0
Option 2: Development of a programme to strengthen the efforts to counter attacks against information systems with non-legislative measures.	-/+	++	-/+	++	A + B ++ C +	-/+
Option 3: Targeted update of FD on attacks to address the threat from large-scale attacks against information systems.	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
Option 4: Introduction of comprehensive EU legislation against cybercrime.	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Preferred option (Options 2 and 3): combination of non-legislative measures with a targeted update of the FD on Attacks	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. HOW DO THE POLICY OPTIONS COMPARE?

6.1. Option (1) Status Quo

This option will inevitably lead to a more vulnerable position of private actors, the Member States and the Union as a whole to deal with cybercrime given its nature and growth. Even at a sustained level of currently existing actions, European coordination would be required.

6.2. Option (2) Development of a programme to strengthen the efforts to counter attacks against information systems with non legislative measures

This option has all the advantages and disadvantages related to a soft law instrument. The positive aspect is a possibility to describe each policy option in a way which is consistent with the best national practices, and thereby facilitate the identification of measures that are best in terms of their effectiveness.

However, this option is less effective in terms of the achievement of the objectives.

6.3. Option (3) Targeted update of FD on attacks to address the threat from large-scale attacks against information systems

This option offers a timely and targeted response to the identified problems. It addresses the criminal law issues necessary to effectively prosecute the perpetrators of this crime. It also improves international cooperation by introducing a mechanism for immediate international assistance in cases of urgent requests for cooperation, and promotes cooperation with the private sector through accompanying measures, such as expert meetings. This option also introduces a number of aggravating circumstances, such as the large-scale aspect of the attacks, as well as attacks committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner.

Finally, to enable measuring of the extent of the problem, monitoring obligations are introduced.

6.4. Option (4) Introduction of comprehensive EU legislation against cyber crime

This option, like option 3, has the added value of establishing binding provisions, and therefore a higher level of effectiveness is expected if fully implemented. It is also expected to maximise the positive impact of both the legislative and non-legislative instruments in a wider range of cyber crime issues than only large-scale attacks. In addition, it would address the criminal law legal framework and at the same time improve law enforcement cooperation over the borders. However, this holistic approach currently at this stage is not reflecting a consensus of stakeholders although its implementation would take the fight against cyber crime a step further than all other options.

7. THE PREFERRED POLICY OPTION

Following the analysis of economic impact, social impact, and impact on fundamental rights, options 2 and 3 present the best approach to the problems with a view to achieving the identified objectives.

Overall, the preferred option would be a combination of policy options 2 and 3, as they complement each other, and therefore best meet the defined objectives, both in substance and timing.

8. MONITORING AND EVALUATION

An implementation report should be published within 2 years after the date of entry into force of the Directive. This report should pay attention to the exact implementation of the Directive by Member States.

Furthermore, regular evaluations should be carried out in order to assess how and to what extent the Directive will have contributed to the achievement of its objectives. The first evaluation should be carried out within 5 years after the entry into force of the Directive; the Commission will then publish evaluation reports every 5 years thereafter and these will include information on implementation. On the basis of the conclusions and recommendations of the evaluations, the Commission should take into account any further amendment to or other possible developments of the Directive.